CEIS

Corporate Executive Information System

Questions or comments related to this plan should be directed to:

Contingency Plan Point of Contact:

Mr. Bob Willis
Executive Information/Decision Support
Phone: 703/575-7467
Email: Robert.Willis@tma.osd.mil

EIDS-Y2K-001

CEIS PROGRAM MANAGEMENT OFFICE

Contingency and Continuity of Operations (COOP) Plan

REVIEW
March 15, 1999

TRICARE
Corporate Executive
Information System

CEIS Program Management Office
5111 Leesburg Pike, Suite 809
Falls Church, VA 22041

EIDS-Y2K-001

Contingency and Continuity of Operations (COOP) Plan

REVIEW

March 15, 1999

Prepared by:

Mr. Richard Shullaw, Date
SRA, International
EI/DS Year 2000 Manager

Reviewed by:

Mr. Robert Willis, GS-1515-12 Date
EI/DS Legacy and Systems Migration Manager
CEIS Program Management Office

Reviewed by:

Mr. Mike Mauro Date
CEIS Systems Architect
CEIS Program Management Office

Approved by:

LTC Carlos Arroyo Date
EI/DS Business Area Technical Manager
CEIS Program Management Office

CEIS Program Management Office
5111 Leesburg Pike, Suite 809
Falls Church, VA 22041

Preface

The Contingency and Continuity of Operations (COOP) Plan provides an overview of how the Program Management Office (PMO) will respond to possible CEIS software problems arising from the crossover to the Year 2000. While CEIS is issuing a Year 2000 compliant release of its software in March 1999, Year 2000 problems can still be encountered, either within the CEIS architecture, as a result of corrupt data received from source systems, or as a result of external events such as massive communications system failures. This document describes the contingencies that have been considered and actions needed to minimize disruption of system operations.

Questions on proposed changes concerning this plan should be addressed to:

CEIS Program Management Office
Legacy Systems and Migration Management
5111 Leesburg Pike, Suite 809
Falls Church, Virginia 22041

Contents

Figures

Section 1: Introduction

1.1 Purpose

The purpose of this document is to provide guidance to the user community in the event the Corporate Executive Information System (CEIS) is unable to process information correctly across the transition to the year 2000. In addition, this plan

- Provides background information on CEIS development efforts
- Provides information on the strategy being followed by CEIS to attain Year 2000 compliance within the deadlines established by Health Affairs
- Defines assumptions being made and alternatives being considered to deal with contingencies and ensure continued, uninterrupted operations by CEIS through the crossover into the Year 2000
- Documents the CEIS Year 2000 programmatic risk assessment
- Presents a project schedule to test and certify the elements of the Year 2000 compliant release of CEIS scheduled implementation in March 1999
- Identifies risk control measures that have been established
- Defines critical path elements within the project schedule
- Establishes a zero-day strategy for programmatic, system, and operational elements of CEIS, along with assigned actions and responsibilities.

1.2 Background

CEIS is a target migration Tri-Service system that integrates data to support decision-making throughout the Military Health System (MHS). The Executive Information/Decision Support (EI/DS) Business Area within Health Affairs provides program management and direction of CEIS. The principal objective of CEIS is to provide timely, accurate, and useful information to hospital and clinic staff, Medical Treatment Facility (MTF) Commanders, Lead Agents, intermediate commands, the Office of the Assistant Secretary of Defense (Health Affairs) [OASD (HA)], and others in the MHS community.

CEIS provides executive decision support information for users at all levels of the MHS. CEIS uses data gathered from a number of source medical information systems. The principal source systems and the information they provide are:

- Composite Health Care System (CHCS) – MHS direct care clinical data
- Ambulatory Data System (ADS) – Direct care outpatient encounter data
- CHAMPUS Source Data Collection System (SDCS) – Outpatient and inpatient records from the Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) program, including those involving the Health Care Financing Administration (HCFA)
- Medical Expense and Performance Reporting System (MEPRS) Executive Query System (MEQS) – Expense, manpower, and workload data from the Expense Assignment System (EAS III and EAS IV)

- Defense Enrollment Eligibility Reporting System (DEERS) – Primary Department of Defense (DoD) source for determining eligibility of military personnel and beneficiary information.

1.3 CEIS Development

CEIS draws information from legacy systems that are managed by the EI/DS Business Area, including the Defense Medical Information System (DMIS) and the Retrospective Case-Mix Analysis System (RCMAS). Valued functionality from these systems is being incorporated into CEIS. As that process is completed, the legacy systems are being shut down. The consolidation of legacy systems into a single migration system (CEIS) provides decision-makers with a national and regional view of health data, and a significant improvement in the currency and accuracy of data available through streamlining of data processing.

The initial CEIS product offering is based on 11 regional databases referred to as the Integrated Databases (IDBs). The IDBs receive data from legacy systems in the EI/DS Business Area, and source systems such as CHCS, DEERS, ADS, MEQS, and SDCS. Two Commercial-off-the-Shelf (COTS) products developed by the HBO&C Company provide the front-end systems for the functional user interface. Trendstar provides detailed patient information for MTF Commanders, allowing them to improve health care service quality and better understanding of health care delivery costs. The second COTS product, Quantum, provides an enterprise view of health care operations to support management decisions and resource allocation. Together, Trendstar and Quantum provide managed care performance measurements, patient cost analyses, and other resource and cost data to support implementation of TRICARE objectives.

The regional database architecture is defined as the CEIS 1.x series. It completed Continental United States (CONUS) deployment in June 1998. This product allows regional and MTF views of beneficiary population, clinical care, enrollment, treatment costing data, and other useful functional data for the Lead Agents and MTF Commanders.

The principal limitation of the CEIS 1.x series is that it provided only a regional view of health care information. DMIS and RCMAS provide views of portions of national level data that is of importance to healthcare decision-makers. To overcome this limitation and meet the needs of corporate level users, the CEIS Program Management Office (PMO) is undertaking development of CEIS 2.0, also referred to as the Enterprise Data Warehouse (EDW). The EDW provides a national level view of health care data for MHS corporate-level managers. Corporate managers include personnel in the Office of the Assistant Secretary of Defense (Health Affairs), the Surgeons General, and intermediate commands.

CEIS 1.x has a distributed computing architecture, whereas CEIS 2.0 will use a centralized computing architecture. The EDW portion of CEIS 2.0 will be hosted on an IBM-SP AIX multi-node processor located at the Defense Information Systems Agency (DISA) megacenter in Denver, Colorado.

The EDW database will use Business Objects software to provide On-Line Analytical Processing (OLAP) capabilities. This provides user flexibility in defining queries, and maintains the correct business relationship of the data during query processing. Data from external sources such as CHCS, DEERS, ADS, and MEQS will be transmitted to the IBM-SP and will then be processed by the Integrated Database Replacement (IDBR) server. The IDBR will prepare data for staging into the EDW database and into other information products, such as the Trendstar and Quantum COTS products. In some cases data will require pre-processing by the IDBR for editing, formatting, and associating values (e.g., associating a catchment area for a specific zip code). The architecture for the EDW and IDBR portions of CEIS 2.0 and a high-level data processing flow for information received from source systems is shown in Figure 1-1.

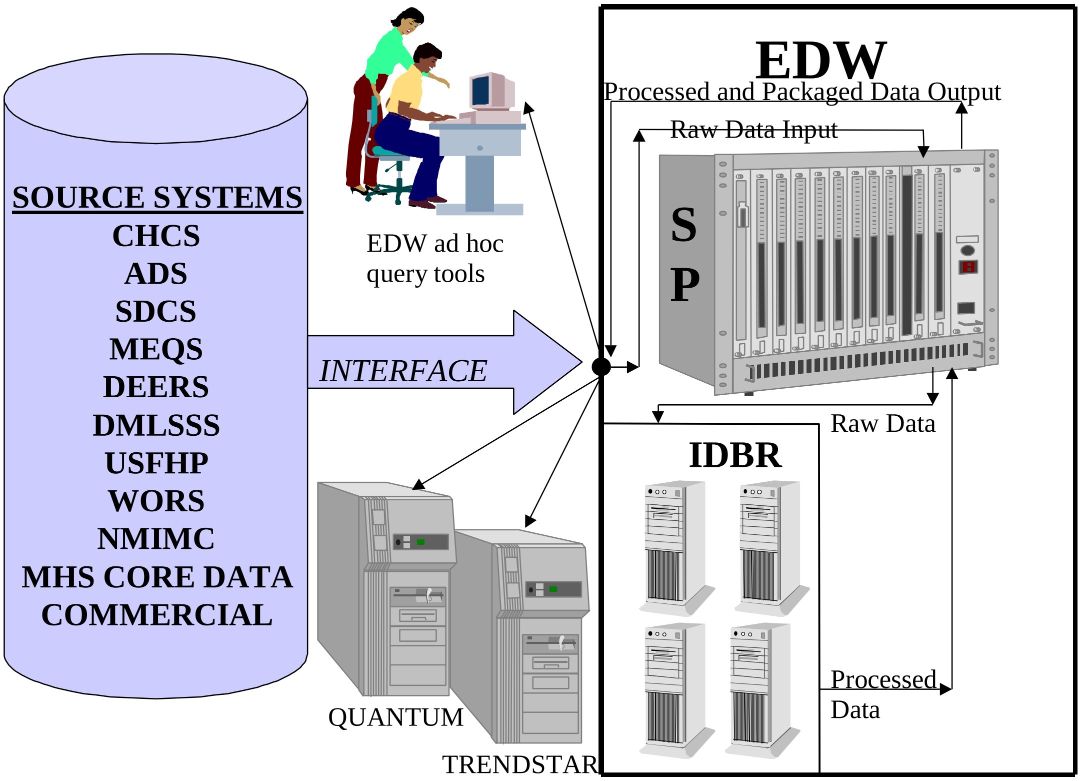

Figure 1-1 EDW and IDBR Architecture, Data Sources

1.4 Applicable Documents

Health Affairs Office of Information Management, Technology and Reengineering, Year 2000 Project Office, Military Health System (MHS) Year 2000 (Y2K) Automated Information System (AIS) Contingency and Continuity of Operations Planning Guide (14 October 1998)

CEIS PMO, CEIS Year 2000 Compliance Plan (Version 1.0, 14 January 1998)

General Accounting Office: Year 2000 Computing Crisis: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19, August 1998)

1.5 Organization and Contents

The remainder of the CEIS Contingency and Continuity of Operations Plan is arranged as follows:

- Section 2 defines the compliance strategy CEIS is following to attain Year 2000 compliance, and the initial program level risk assessment
- Section 3 describes the implementation schedule for the Year 2000 compliant release of CEIS, and the critical path analysis associated with the implementation schedule
- Section 4 outlines the system level contingency plan for CEIS
- Section 5 specifies the zero-day strategies at the program, system and operational levels that will be followed by CEIS to minimize the impact of any unforeseen problems that occur during fiscal or calendar year crossover to 2000.

Section 2: Compliance Strategy

As described in Section 1, CEIS is the target migration system for all AISs within the EI/DS Business Area. As part of that migration effort, the EDW is being developed as the cornerstone of CEIS 2.0. Because CEIS 2.0 will not be operational until the 4th Quarter of Fiscal Year (FY) 1999 or later, CEIS is taking action to make the current fielded version Year 2000 compliant by the 31 March 1999 MHS and DoD deadline. This section describes the compliance strategy being followed, and the initial program level risk assessment of that strategy.

2.1 CEIS Year 2000 Compliance Strategy

The currently fielded version of CEIS (Release 1.7) is not year 2000 compliant. Non-compliant elements are the IDBs and the currently fielded version of Trendstar and Quantum (v.98.1). In addition, DMIS and RCMAS are not Year 2000 compliant.

CEIS 2.0 has been designed to be Year 2000 compliant. This includes all hardware and software elements used by the EDW and the IDBR. All dates in the EDW are stored in four-digit year format. The IDBR is supported by software that allows it to correctly interpret any two-digit year dates it may receive from source systems.[1] However, CEIS 2.0 will become operational no earlier than the 4th Quarter of FY 1999.

DoD Health Affairs has classified CEIS as a Mission Essential information system. The Health Affairs deadline for deploying Year 2000 compliant versions of Mission Essential systems is 31 March 1999. Because CEIS 2.0 will not be operational until after that deadline, EI/DS is taking steps to make the next release of CEIS (Release 1.8) Year 2000 compliant by the Health Affairs deadline.

The strategy being followed by the PMO is to ensure that non-compliant portions of CEIS are either repaired or shut down. The CEIS Development Test and Evaluation (DT&E) staff will perform independent verification and validation (IV&V) of Year 2000 compliance of the components of CEIS 1.8. In addition, the PMO is following a strategy to ensure that core data and residual processing performed by DMIS and RCMAS are made Year 2000 compliant and are migrated to a Year 2000 compliant environment. Table 2-1 summarizes the issues involved in achieving Year 2000 compliance, the planned remediation, and the scheduled completion date for each element of the strategy. Those dates shown in **bold** indicated completed actions. The table is updated as of 12 March 1999.

Table 2-1. CEIS 1.8 Year 2000 Compliance Strategy Issues

ISSUE	CORRECTIVE ACTION	PLANNED FINISH DATE
IDBs not Year 2000 compliant	Replace IDBs with Y2K compliant IDBR capability 1. Begin operations with initial IDBR in Region 11. 2. Shutdown IDB in Region 11. 3. Complete replacement of IDBs in remaining regions.	**1. 19 February 1999** 2. NLT 10 April 1999 3. NLT 30 June 1999

[1] Some dates received from CHCS are in two-digit year format. An example is the MTF Admission Date found in the Standard Inpatient Data Record (SIDR).

ISSUE	CORRECTIVE ACTION	PLANNED FINISH DATE
Fielded versions of Trendstar and Quantum (v98.1) are not Year 2000 compliant	1. HBOC repairs software. 2. DT&E completes acceptance testing, approves release to the regions. 3. DT&E completes Y2K testing. 4. Complete installation in all regions.	**1. 15 November 1998** **2. 2 February 1999** **3. 26 February 1999** 4. 15 March 1999
CEIS All-Region Server (ARS) not Year 2000 compliant	1. Upgrade UNIX Operating System (OS) and Informix database to Year 2000 compliant versions. 2. Complete Y2K testing. 3. Begin operations with compliant version of ARS.	**1. 31 January 1999** **2. 28 February 1999** 3. 15 March 1999
IDBR has not been tested for Year 2000 compliance	1. Begin IDBR operations in Region 11 to validate operational capability. 2. Complete Y2K testing of IDBR.	**1. 19 February 1999** 2. 22 March 1999
SP2 has not been tested for Year 2000 compliance	1. Establish test environment. 2. Complete Y2K testing of SP2.	**1. 1 March 1999** 2. 15 March 1999
Managed Care Forecasting and Analysis System (MCFAS) operating system and data base are not Year 2000 compliant[2]	1. Upgrade UNIX operating system and Informix database. 2. Complete Y2K testing.	**1. 8 January 1999** **2. 14 February 1999**
DMIS and RCMAS are not Year 2000 compliant.	1. Develop Software Change Requests (SCRs) to determine areas of Year 2000 non-compliance, and level of effort required repairing the systems and making them Year 2000 compliant. 2. Identify key residual functions that provide critical support to corporate MHS responsibilities identified.[3] 3. Develop strategy to migrate residual functions from non-Y2K compliant Sequent computer to Year 2000 compliant DEC ALPHA 4100 and IBM Mainframe at Ft. Detrick. 4. Complete migration of residual functions. 5. Shutdown DMIS and RCMAS.	**1. 30 September 1998** **2. 15 December 1998** **3. 11 February 1999** 4. 1 May 1999 5. 30 June 1999

2.2 CEIS Program Level Year 2000 Risk Assessment

In October 1997, the CEIS PMO established a CEIS Year 2000 Workgroup under the direction of the CEIS Legacy Systems and Migration Manager. The workgroup includes

- Operators and developers of the CEIS 1.x series
- Developers of CEIS 2.0
- Managers and operators of legacy systems to be migrated to CEIS

[2] MCFAS is a replacement system for the Resource Analysis and Planning System (RAPS), which ceased operations in November 1998.

[3] Examples of these functions include population processing and Bid Price Adjustment (BPA)

- Managers of other information systems in the EI/DS Business Area, including the Defense Medical Surveillance System (DMSS), MCFAS, and SDCS
- CEIS Year 2000 program support staff
- Year 2000 testers.

The workgroup meets on a weekly basis, and has analyzed the Year 2000 compliance status of CEIS, tracing data flows and data structures from source systems through CEIS processing to user display. The CEIS Year 2000 Workgroup found substantial Year 2000 problems in Quantum and Trendstar during their initial assessment leading to the remediation effort summarized in Table 2-1. The workgroup developed a schedule for remediation of identified problems, and, working with the CEIS Test and Evaluation Workgroup (TEWG), established Year 2000 test requirements for remediated and new elements of the CEIS architecture. The compliance strategy issues shown in Table 2-1 are a result of ongoing discussions between the Year 2000 Workgroup and the TEWG.

Table 2-2, shown on this and the following page, displays the high level programmatic risk assessment required by Health Affairs as part of the contingency planning process. The table is separated into sections dealing with cost, schedule, performance, and technical risk evaluation. The table indicates that CEIS faces low risks in meeting program deadlines. Standing alone, this assessment does not provide a complete picture of risks related to meeting the MHS deadline of 31 March 1999 for Year 2000 compliance of mission essential information systems.

Table 2-2: CEIS Programmatic Risk Assessment

Y2K PROGRAMMATIC RISK ASSESSMENT QUESTIONNAIRE	
AIS: Corporate Executive Information System (CEIS)	**Date: 3 February 1999**
Cost Risk Evaluation	
1. Is the renovation of the system or replacement system fully funded? **YES** 2. Does the funding include the deployment, testing, implementation, training, and conversion of the new or renovated system? **YES** 3. Is the cost of ensuring Y2K compliance of the operating system/executive software and hardware funded? **YES** 4. Are all interfaces (internal and external) identified, and is sufficient funding earmarked to ensure renovation, testing, and certification, as required? **YES** 5. Are contingency funds available to cover unanticipated renovation, testing, and/or implementation issues?	
Renovation requirements were identified during initial assessment of CEIS compliance level	
Rating: High Risk Medium Risk **LOW RISK**	

Schedule Risk Evaluation

1. Are all DoD and MHS mandated phase milestones achieved? **YES. In validation (testing) phase.**
2. Is the implementation going to be achieved within the DoD and MHS mandates? * **YES**
3. Are testing and rework activities factored into the schedule? **YES**
4. Are interface renovations/development (internal and external) factored into the schedule? **YES**
5. Is sufficient time scheduled for interface testing, rework, and certification? **YES**
6. Are there significant schedule interdependencies with other AIS projects? **NO**
7. Are there significant interdependencies with system software, hardware, or infrastructure elements? **NO**
8. Are COTS vendor schedules adequate to meet DoD and MHS requirements? **YES**
9. Is a master program schedule network developed in an automated project management tool? **YES**
10. Is a critical path identified, and has critical path analysis been performed? **YES**

Note: If the answer question 2 is NO, schedule risk must be classified as “High.”

Rating: High Risk Medium Risk **LOW RISK**

Performance/Technical Risk Evaluation

1. Has a formal Y2K Project Plan been prepared, approved, and published? **YES**
2. Does the project plan address system software and system-to-system interfaces? **YES**
3. Does the plan address local area/wide area communications? **YES**
4. Does the plan address data conversion, testing, training, and certification requirements? **YES**
5. Is the local area communications system (LAN) compliant? **YES**
6. Does the plan include procedures for ensuring Y2K compliance of system software and hardware? **YES**
7. Does the plan call for system-level testing to include COTS products and internal and external interfaces? **YES**

Rating: High Risk Medium Risk **LOW RISK**

The CEIS Year 2000 Workgroup has focused on specific risk identification and mitigation measures leading to implementation of CEIS 1.8, the Year 2000 compliant release, in March 1999, and shutdown of DMIS and RCMAS by the end of June 1999.[4] A summary of the principal risks identified and the mitigation strategies adopted are shown in Table 2-3. Dates shown in parentheses reflect completed actions.

Table 2-3: Risk Identification and Mitigation Measures for CEIS 1.8 and Shutdown of DMIS and RCMAS

RISK	MITIGATION
Performance/Technical Risks	
HBOC 98.1 software determined to be non-compliant through analysis of data flows into and through the IDBs.	• Work with vendor to define deficiencies and determine schedule for delivery of corrected software (May 1998). • New version of software developed (98.2) and delivered to PMO (November 1998). • Perform Year 2000 testing to ensure problems have been corrected (February 1999).
Data analysis determined IDBs are non-Y2K compliant, and that replacement costs would negatively impact program development.	• Develop IDBR capability to replace IDBs • Begin IDBR operations in Region 11 (February 1999). • Replace remaining IDBs with IDBRs.

[4] With implementation of CEIS 2.0 now scheduled for September 1999, the Year 2000 Workgroup expects to identify additional risks and mitigation strategies applicable to that release. Those risks will be documented in Version 1.1 of the CEIS Contingency and Continuity of Operations Plan.

RISK	**MITIGATION**
Performance/Technical Risks	
The new DEERS extract will not be delivered until at least June 30, 1999. The IDBR is designed to use the new DEERS extract to support CEIS population processing.	• Develop capability for IDBR to handle old and new DEERS extracts. • Migrate population processing that relies on the DEERS extract to Y2K compliant DEC ALPHA platform.
Shutdown of DMIS and RCMAS leaves risk that key residual processes needed by MHS are not supported. Key example is Bid Price Adjustment (BPA).	• Correct Y2K problems in residual processing code • Port corrected residual processing code from DMIS/RCMAS to DEC ALPHA. • Establish directory structure on IBM Mainframe at Ft. Detrick to support SAS datasets, MEPDRG, etc. • Shutdown DMIS and RCMAS GUI during the Third Quarter, FY 1999.
HBOC v98.2 fails Y2K testing.	• Continue v98.2 in regions until HBOC makes repairs • If repairs and Y2K retesting not completed by 1 August 1999, implement procedures to store source system data that populates HBOC. • Respond to critical user data needs through use of information in SAS data sets.
IDBR fails Y2K acceptance testing.	• Maintain current IDB architecture until 30 June 1999. • If IDBR remains non-operational, establish backup procedures with source systems to store relevant data until IDBR becomes operational.
SP2 fails Y2K acceptance testing because of problems with the AIX operating system	• Develop action plan with IBM to correct situation • Maintain IDB architecture until 30 June 1999. • If SP2 remains non-operational, establish backup procedures with source systems to store relevant data on Y2K compliant IBM mainframe at Ft. Detrick until SP2 becomes operational.

.

Section 3: CEIS Implementation Schedule

This section describes the implementation schedule being followed for CEIS Release 1.8 to achieve the 31 March 1999 MHS Year 2000 compliance deadline. To provide a more comprehensive picture, details of the implementation schedule for CEIS 2.0 are also included. This section concludes with a description of the critical path analysis performed in conjunction with the fielding of Release 1.8.

3.1 Implementation Schedule

The PMO maintains a master integrated project schedule that covers all of the implementation tasks involved with CEIS Release 1.8. The project schedule includes tasks for implementation of CEIS Release 2.0 in September 1999. The project schedule is managed through use of Primavera scheduling software, and is updated at weekly CEIS Status Review Board (SRB) meetings. The updated schedules are distributed to all key staff involved in CEIS development, testing, maintenance, and administration staff, in addition to management staff in the PMO. Risk assessments are performed to evaluate the impact of any schedule delays, the effect on related tasks, and the alternatives available for corrective action.

The schedule covers several hundred tracked items. Given the complexity of the CEIS implementation effort, it is subject to frequent changes. Table 3-1 provides a high level view of the principal dates to implement and certify CEIS Release 1.8 as Year 2000 compliant. The table also provides a high level view of the actions and schedule for recertifying CEIS 2.0 as Year 2000 compliant.

Table 3-1: Principal CEIS Year 2000 Milestones

EVENT	COMPLETE BY
CEIS 1.8	
Year 2000 testing of ARS	28 February 1999
Year 2000 testing of MCFAS	17 February 1999
Year 2000 testing of HBOC 98.2	26 February 1999
Year 2000 testing of IDBR	22 March 1999
Year 2000 testing of SP2	15 March 1999
Consolidated Y2K test report on ARS, MCFAS, HBOC, IDBR, and SP2	24 March 1999
Preparation of Y2K certification material	26 March 1999
Submission to CEIS Program Manager for review and approval	28 March 1999
Certification package submitted to MHS Y2K Project Officer	30 March 1999
CEIS 2.0	
Year 2000 testing of CEIS 2.0	TBD
Preparation of CEIS 2.0 Year 2000 recertification material	TBD
Submission to CEIS Program Manager for review and approval	TBD
Recertification package submitted to MHS Y2K Project Officer	TBD
GIAT for CEIS 2.0	30 July 1999
Obtain OT IPT Milestone IIIB approval	13 September 1999
Commence operations with Year 2000 compliant CEIS 2.0	30 September 1999

3.2 Critical Path Analysis

Critical Path Analysis (CPA) has been performed to ensure that schedule risks and contingencies are identified and viable plans and workarounds are developed to address possible schedule delays. Critical activities are defined as those that must be completed on time to prevent delays that would impact the ability to meet the MHS and DoD deadline of 31 March 1999 for Year 2000 compliance and certification. Through the ongoing use Primavera scheduling software, the PMO is able to continuously assess the impact of any task delays on overall schedule completion. In addition, the Primavera tool has allowed the PMO to consider and adopt alternatives to attaining Year 2000 compliance. For example, the PMO was able to rapidly implement an alternative approach to the handling of population data when delays in implementation of the new DEERS extract were encountered[5]. The PMO was able to establish an alternative strategy for handling population data feeds from source systems.

The critical path information shown in Table 3-2 provides a picture of analysis performed as of the date of writing this contingency plan. Because this analysis is a regular activity at the weekly Status Review Board meetings, CPA is an ongoing process.

Table 3-2: Critical Path Analysis

Legend:

P	probability of occurrence	L = Low
C	consequences of occurrence	M = Medium
RC	risk classification	H = High

<table>
<tr><th colspan="5">COMPLETED CRITICAL MILESTONES</th></tr>
<tr><th colspan="4">Critical Activity</th><th>Completed</th></tr>
<tr><td colspan="4">Year 2000 assessment phase</td><td>30 June 1998</td></tr>
<tr><td colspan="4">Complete Year 2000 compliance plan</td><td>14 January 1998</td></tr>
<tr><td colspan="4">Complete Interface Agreements with source systems</td><td>15 June 1998</td></tr>
<tr><td colspan="4">Complete initial CEIS IV&V Review</td><td>14 October 1998</td></tr>
<tr><td colspan="4">Complete Year 2000 test plans for ARS, HBOC, MCFAS</td><td>15 January 1999</td></tr>
<tr><td colspan="4">Complete Year 2000 testing of MCFAS</td><td>17 February 1999</td></tr>
<tr><td colspan="4">Begin operations of IDBR in Regions 3 and 11</td><td>26 February 1999</td></tr>
<tr><th colspan="5">IDENTIFYING CRITICAL PATH ELEMENTS AND DOCUMENTING THE RESULTS OF THE ANALYSES</th></tr>
<tr><th>Critical Activity</th><th>P</th><th>C</th><th>RC</th><th>Risk Mitigation Procedures</th></tr>
<tr><td>Perform Year 2000 testing of ARS</td><td>L</td><td>L</td><td>L</td><td>Upgrades to O/S and Informix complete. Y2K testing in progress with no identified problems: to be completed 2/28/1999. If Y2K testing fails, remediation is to isolate ARS data from users.</td></tr>
<tr><td>Perform Year 2000 testing of HBOC 98.2</td><td>M</td><td>H</td><td>H</td><td>Y2K testing to be completed 2/27/1999. Y2K problem identified in Quantum affecting displays, but not affecting accuracy of data after rollover. Working with HBOC to make fixes. High risk because limited time available to complete testing of fixes.</td></tr>
<tr><td>Perform Year 2000 testing of IDBR</td><td>L</td><td>H</td><td>M</td><td>Y2K testing covers operating system (Windows NT) and DataStage software. Y2K testing to complete 3/22/1999. Limited scope of testing and Y2K compliance of individual elements of the IDBR mitigates risk.</td></tr>
<tr><td>Perform Year 2000 testing of SP2</td><td>L</td><td>M</td><td>M</td><td>Y2K testing covers only the AIX operating system and supporting system administration tools. Y2K testing to complete 3/15/1999. Limited scope of testing and Y2K compliance of AIX mitigates risk.</td></tr>
</table>

[5] DEERS has indicated that the new extract will not be implemented before the end of June 1999. This delay is outside the span of control of the CEIS PMO, but must be dealt with as CEIS 1.8 is implemented.

IDENTIFYING CRITICAL PATH ELEMENTS AND DOCUMENTING THE RESULTS OF THE ANALYSES				
Critical Activity	P	C	RC	Risk Mitigation Procedures
Perform CEIS contingency plan testing	L	L	L	Testing and refinement of contingency plan procedures to begin April 1999 after initial establishment of IDBR operational capability, and certification of CEIS Release 1.8
Shutdown IDBs in Regions 3 and 11	M	H	H	Parallel data feeds to IDBR and IDB in Regions 3 and 11 during February and March 1999. If feeds to IDBR are successful, shutdown IDBs in Regions 3 and 11 in April 1999. If feeds to IDBR are not successful, feeds to IDBs are primary data source until IDBR becomes operational.
Deploy additional IDBRs to Denver Megacenter	L	L	L	Additional IDBRs are on hand and being configured for placement in Denver Megacenter.
Shutdown IDBs in remaining regions	M	H	H	Parallel data feeds for IDBs and IDBR in remaining regions during March and April. If successful, shut down remaining IDBs in May 1999. If feeds to IDBR are not successful, continue feeds to IDB until IDBR becomes fully operational.
Develop capability to handle residual processes now performed by DMIS and RCMAS	M	M	M	Residual processes have been identified and are being corrected for Y2K problems identified during assessment phase compliance effort. User access to DMIS and RCMAS to be shut off 31 March 1999. Residual processes to be ported to Y2K compliant environment by end of May 1999.

Section 4: System Level Contingency Plan

This section provides a broad overview of the system level contingency plan developed to support response to contingency situations. The plan is supplemented by more specific discussion of zero-day strategies that will be in place to support response to unanticipated system problems immediately before, during, and after the crossover to the next millennium.

4.1 System Level Contingency Plan

CEIS is establishing procedures to ensure that operations staff, system administrators and help desk personnel are prepared to handle any Year 2000 problems that may arise just before, during, and after the crossover to the Year 2000. The Failure Time Horizon (FTH) established to be ready to implement procedures shown in Table 6 is Monday 27 September 1999, three days before the end of Government FY 1999. CEIS makes extensive use of Fiscal Year calculations, projections, and displays of data. The PMO wants to be ready to respond swiftly to any problems that arise as FY 2000 begins. That response capability will remain in place in the period immediately before, during, and after the crossover to Calendar Year (CY) 2000.

A Help Desk located in San Antonio, Texas supports the CEIS program. The Help Desk answers questions about CEIS functions, and assists users in developing tailored report formats to meet specialized program and costing analysis requirements. The Help Desk has comprehensive understanding of CEIS and its data, and is also familiar with the operation and capabilities of legacy systems such as DMIS and RCMAS. The Help Desk will play a major role in responding to system level Year 2000 problems that may be encountered.

In addition to the Help Desk, the PMO will make extensive use of CEIS System Administrators (SAs) as part of the response chain if system-wide Y2K problems occur. A CEIS SA is located in each of the eleven regions. Their current responsibilities involve the orderly transfer of data from the IDBs to the Regional Datamarts, which consist of the HBOC Trendstar and Quantum servers. The replacement of the IDBs with the IDBR capability leaves intact the responsibility of the SAs to transfer data to the Regional Datamarts. The SAs therefore provide an additional level of support that can rapidly respond to any system level problems that may arise. The PMO will also work with the Tri-Service Infrastructure Management – Program Office (TIMPO) to deal with any network communications issues that arise. The PMO has worked extensively with TIMPO staff to establish the network CEIS uses to support its user community.

CEIS system level contingency planning includes procedures to report, analyze, repair, test and distribute repaired software to the user community in the event system wide Year 2000 failures occur. Table 4-1, shown on the following page, delineates the risks, the consequences of system malfunction or failure, and the course of action that will be taken to minimize the impact of Year 2000 problems on normal operating procedures. The table is separated into four sections:

- Problem identification
- Problem analysis
- Software repair and problem resolution
- Repaired software and hardware distribution

Additional details of the contingency approach being followed by CEIS are found in Section 5 – Zero-Day Strategies.

Table 4-1: System Level Contingency Plan

Legend:

P	probability of occurrence	L = Low
C	consequences of occurrence	M = Medium
RC	risk classification	H = High

NORMAL OPERATING PROCEDURES	Y2K RISK	P	C	RC	CONTINGENCCY OPERATIONS MODE
Problem Identification					
User reports problem to CEIS Help Desk	Help desk unable to resolve problem.	L	H	M	User instructed to maintain record of operation performed and error encountered, including screen prints to show Y2K problem. Help Desk provides contingency operating mode instructions to user (manual operating procedures).
Help Desk reports problem to System Administrator (SA)	SA unable to resolve problem.	L	H	M	User continues manual operating mode pending problem resolution.
SA reports problem to PMO	SA unable to resolve problem.	L	H	M	Users notified of problem and instructed to implement available manual operating procedures.
Problem Analyses					
PMO refers problem to support staff to analyze and develop solution	Support staff unable to resolve problem.	L	M	M	Assemble Integrated Contractor Team (ICT) to analyze problem, develop solution.
PMO determines problem is caused by failure of system interface	Support staff of involved system unable to develop timely solution.	L	M	H	Work with involved system to store data off-line until problem is corrected. Advise users that data will not be available until problem is corrected.
PMO determines problem is result of corrupt data received from source system	Source system unable to resolve problem in timely manner.	M	M	M	Implement backup procedures to store source system data off-line until problem is corrected. Advise users data involved will not be available until problem corrected.
CEIS PMO coordinate response to non-software problems (hardware, local, wide-area communications) with vendors, TIMPO, and SAs as needed	Response entities unable to develop timely solution to problem.	L	M	M	Isolate those portions of the system that are affected by the non-software problem. Make arrangements with affected source systems to store data off-line until problem is corrected. Notify users of the extent of the problem, and the anticipated correction schedule.
Software Repair/Problem Resolution					
Software is repaired and tested, provided to SAs for implementation	Repaired software does not correct problem in field because of hardware or communications problems.	L	M	M	Work with hardware and communications organizations including TIMPO to further analyze and correct problem. Advise users of new schedule when developed.
Software is repaired and tested provided to SAs for implementation	Unable to resolve, system software issue.	L	M	M	Exercise repair agreements with vendors and develop schedule for implementation of correction. Backup data as needed at source system level.

NORMAL OPERATING PROCEDURES	Y2K RISK	P	C	RC	CONTINGENCCY OPERATIONS MODE
Software/Hardware Distribution					
Vendor repairs hardware and implements fix	Vendor unable to deliver because of multiple Year 2000 problems.	L	M	M	Backup data as needed at source systems. Develop alternative strategies to bypass the affected hardware.

Section 5: Zero-Day Strategies

The PMO is faced with dual challenges of implementing a Year 2000 compliant release of CEIS in March 1999, and continuing development of CEIS 2.0 for implementation in the field no earlier than the last quarter of CY 1999. The PMO is committed to ensuring that Year 2000 problems do not limit the ability of CEIS to deliver critically needed health care information to the MHS community. Strong management support and immediate response to worst case scenarios that could occur during the millennium crossover will implement this commitment. The foundation of the effort will be clear, unambiguous and ongoing communication with the user community at the MTF, Lead Agent, Headquarters, and corporate level.

This section describes zero-day strategies that will be followed by CEIS at the time of the calendar and fiscal year crossovers to the next millennium. The section is separated into programmatic, system, and operations guidelines that will be used as a baseline to develop additional, detailed operating procedures.

5.1 Programmatic Strategies

Table 5-1. Programmatic Zero-Day Strategies

Objective: **The CEIS PMO will be ready to provide responsive management and control of worst case scenarios before, during and after 1 October 1999 and 1 January 2000.**	
Planning Element	Elements of Zero-Day Strategy
Budget Requirements	• The CEIS PMO will establish the quantity and type of personnel and material requirements needed from government and contractor personnel. • The budget needed to support this effort will be compared to available funds. • Where a shortfall would impact the ability of CEIS to respond to anticipated emergency scenarios, additional funding will be sought from Health Affairs Y2K contingency funds. • The PMO will develop and coordinate with their contractors stand-by task orders that cover Y2K repair efforts that occur immediately before and after the millennium crossover.
Staff Resources	• From September 15 to October 15, 1999, and from December 17, 1999 to January 15, 2000, annual leave for key CEIS PMO staff will be staggered to ensure continuous coverage of critical functions such as operations, help desk, training, and deployment. • The CEIS PMO will work through the ICT to ensure that key staff from the development and operations contractors are available throughout the period described above.
System and Data Integrity	• The PMO will ensure that a full back-up of the CEIS system and data occurs by 15 September 1999 to deal with the FY 2000 crossover, and again by December 15 1999 to deal with the CY 2000 crossover. At least two copies of the backup will be made.
Coordination with source data systems	• The PMO will work with the source systems from which CEIS receives data to ensure that provisions of already completed Interface Agreements (IAs) are reviewed, and that addendum are prepared as needed to support zero-day strategies. These systems include DEERS, CHCS, MEQS, ADS, and SDCS.
Ongoing communication with the user community	• The PMO will develop an overall policy document to define how communication will be handled between the various types of CEIS users at the MTF, Lead Agent, Headquarters, and corporate level, the Help Desk, and designated key PMO personnel. This policy will be communicated through the Advocate, Expresso, and the CEIS web site. • The PMO will distribute a current Pont of Contact (POC) list to the user community by 31 August 1999. • The PMO will include articles in the Advocate and Expresso describing possible and actual Y2K problems CEIS or source systems on which it relies for data are encountering. These articles will begin in June 1999.
Project schedules	• The user community will be provided with instructions on how to access to CEIS project schedule included in the Integrated Program Planning Scheduling and Reporting System (IPPSRS).

5.2 System-Level Strategies

Table 5-2. System Level Zero-Day Strategies

Objective: **The CEIS PMO will ensure resources are available to expeditiously identify, report, accept, and correct systems problems before, during and after 1 October 1999 and 1 January 2000.**	
Planning Element	Elements of Zero-Day Strategy
User access to knowledgeable staff	• The PMO will develop procedures with the Customer Service Division (CSD) Help Desk and the Tri-Service Medical Systems Support Center (TMSSC) to provide extended customer support during key periods immediately before and after the millennium crossover (September 15 to October 15, 1999, and December 17, 1999 through January 15, 2000). • The PMO will work with TMSSC and CSD to establish problem-reporting procedures that ensure the customer is informed of progress in resolving Y2K problems. • The PMO will add customer support information tailored to Y2K issues to the CEIS web page, including means to allow users to directly enter problem reports through use of the web page. • The PMO will work with contractors responsible for the regional System Administrators to ensure extended coverage during the time periods defined above to deal with any system problems at the Regional Datamarts.
Notice to users of problems	• The PMO will establish multiple means to notify users of system problems, the schedule for their correction, and any steps that need to be taken by users to minimize or alleviate their impact. • The PMO will test notification methods during August 1999 as part of the overall test of contingency plan procedures.
ICT response to system problems	• The PMO will ensure effective coordination of system repair activities through use of the ICT. • The CEIS Executive Program Manager or a designated government representative will chair work sessions of the ICT. • The ICT will establish Emergency Response Teams (ERT) that can be deployed to correct Y2K problems encountered at regional sites or at the Denver Megacenter. The teams will include programmers, system administration specialists, and functional experts as needed.
Establishing joint repair strategies with source data systems	• Where the system problem involves data received from a source system, the PMO will activate provisions of existing IAs to ensure development of a coordinated response. • As a first step, the response effort will include development of a project schedule with clear assignment of responsibilities, and a timeline for completion and joint testing of the repaired elements.
Budgetary requirements	• Working with the ICT and source systems, the PMO will develop cost figures to effect repairs immediately after the problem is identified, and to support deployment of ERTs when necessary. • Where funds are not available within the CEIS or source system budget to make the needed repairs, the PMO will quickly prepare documentation to support request for HA contingency funding. The documentation will include the impact on MHS operations if the repairs are not made.

Planning Element	Elements of Zero-Day Strategy
Problem data collection	• Health Affairs will be required to report the extent of information systems Y2K problems to OSD (C3I), and the status of efforts to correct or minimize those problems. • To support Health Affairs, the PMO will establish procedures, gather data from users, SAs and the Help Desk on problems encountered, remediation efforts, and expected resumption of normal operations. The PMO will use this data to develop cost figures for repairs and implementation of contingency procedures.

5.3 Operational Strategies

Table 5-3. Operational Level Zero-Day Strategies

Objective: **The PMO will ensure that it provides support needed by the user community to respond to Y2K incidents that may affect the operation of CEIS.**	
Planning Element	Elements of Zero-Day Strategy
On-site resources	• The PMO will be prepared to deploy staff (government and contractor) to remote sites to support operations during the millennial crossover. The principal site to which the staff will be deployed is the Denver Megacenter. • The PMO will be prepared to deploy ERTs when Y2K problems occur that have a major impact on CEIS operations.
Coordination with contractor staff	• Through the ICT, the PMO will ensure that Y2K problems that affect operations are immediately communicated to contractor staff. • The PMO will work with contractor staff to ensure that the right mix of expertise is provided to staff the ERTs.
Communicating with the user community	• The PMO will ensure that the status of system performance is promptly communicated to the user community. This will include notice of problem areas, the schedule for repair, and the implementation of new software or procedures to deal with the problems. • The PMO will ensure that implementation of manual operating procedures, or return to automated procedures after a system failure are promptly communicated to the user community. This includes provisions for a positive acknowledgement by the users of this information. • The PMO will make use of multiple channels of communication (Help Desk, TMSSC, CEIS Web Site, Expresso, e-mail, and faxes) in case Y2K problems are encountered in one or more of the communications channels. • The PMO will establish procedures with the ICT to ensure that progress on Y2K remediation efforts is included in monthly reports.
Interface with source data systems	• The PMO will work with source data systems to establish a schedule and conduct Y2K testing of data exchanges after implementation of CEIS 1.8 in March 1999. • Working with the Interface Working Group (IWG) established with each source system, the PMO will review contingency plans and procedures to ensure that roles and responsibilities are understood, and resource allocations are in place. • The PMO will schedule joint contingency plan testing with source data systems during the 3rd Quarter, FY 1999. Results of those tests will be used to refine plans, procedures and budget requirements.
Monitoring efficiency of manual operations	• Manual procedures implemented by the PMO as a result of system failure will be monitored and analyzed for efficiency. • Any changes to procedures resulting from this effort will be promptly communicated to the user community.
Reporting and data gathering	• To respond to HA and OSD (C3I) reporting requirements, a log will be maintained at the Denver Megacenter, the CEIS regional sites, and the Help Desk to record receipt and description of Y2K problems. • The PMO will be responsible for consolidating this data and providing reports as needed to HA and OSD (C3I). • Problem report data will be provided to the user community to keep them informed of overall system performance, and the schedule for remediation of any substantial problem areas.

Appendix A: Glossary of Abbreviations

ADS	Ambulatory Data System
AIS	Automated Information System
ARS	All Region Server
BPA	Bid-Price Adjustment
CHAMPUS	Civilian Health and Medical Program of the Uniformed Services
CHCS	Composite Health Care System
CEIS	Corporate Executive System
CONUS	Continental United States
COOP	Continuity of Operations
COTS	Commercial off the Shelf
CPA	Critical Path Analysis
CY	Calendar Year
DEC	Digital Equipment Corporation
DEERS	Defense Enrollment Eligibility Reporting System
DISA	Defense Information Systems Agency
DMIS	Defense Medical Information System
DMSS	Defense Medical Surveillance System
DoD	Department of Defense
DT&E	Development Test and Evaluation
EDW	Enterprise Data Warehouse
EI/DS	Executive Information / Decision Support (Business Area)
ERT	Emergency Response Team
FTH	Failure Time Horizon
FY	Fiscal Year (Government)
GAO	General Accounting Office
HA	Health Affairs
HBOC	HBO&C Company
HCFA	Health Care Financing Administration
IA	Interface Agreement
ICT	Integrated Contractor Team
IDB	Integrated Database
IDBR	Integrated Database Replacement (Server)
IPPSRS	Integrated Program Planning Scheduling and Reporting System
IV&V	Independent Verification and Validation
IWG	Interface Working Group
MCFAS	Managed Care Forecasting and Analysis System
MEQS	Medical Expense and Performance Reporting System (MEPRS) Executive Query System (MEQS)
MHS	Military Health System
MTF	Medical Treatment Facility
OASD(HA)	Office of the Assistance Secretary of Defense (Health Affairs)
OLAP	On-Line Analytical Processing
OS	Operating System
OT IPT	Overarching Technology - Integrated Product Team
PMO	Program Management Office
POC	Point of Contact
RAPS	Resource Analysis and Planning System
RCMAS	Retrospective Case-Mix Analysis System
SA	System Administrator
SCR	Software Change Request
SDCS	Source Data Collection System
SIDR	Standard Inpatient Data Record
SP-2	IBM Hardware used for the EDW

SRB	Status Review Board
TEWG	Test and Evaluation Work Group
TIMPO	Tri-Service Infrastructure Management Program Office
TMSSC	Tri-Service Medical Systems Support Center
TRICARE	Tri-Service Health Care
Y2K	Year 2000